No. 05-424

In The

Supreme Court of the United States

RAJIB K. MITRA,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For A Writ Of Certiorari To The United States Court Of Appeals For The Seventh Circuit

PETITION FOR A WRIT OF CERTIORARI

ROBERT G. LEBELL
KOSTICH, LEBELL, DOBROSKI & MORGAN LLP
735 West Wisconsin Avenue, #800
Milwaukee, WI 53233-2413
Phone: (414) 276-1233
Fax: (414) 276-5874
Email: dorbell@execpc.com

COCKLE LAW BRIEF PRINTING CO (800) 225-6964
OR CALL COLLECT (402) 342-2831

QUESTIONS PRESENTED

1. Whether broadcasting radio signals that interfere with police radio communications is properly subject to prosecution under 18 U.S.C. § 1030, which is titled "Fraud and related activity in connection with computers." The statute had previously been invoked solely to prosecute computer hacking. In reaching its decision, the Seventh Circuit Court of Appeals held that legislative intent is not relevant where the statutory language may be broadly read to permit criminal prosecution in novel factual scenarios.

2. Whether the Seventh Circuit's procedure of employing a limited remand to district courts for the purpose of having the district court decide, without a re-sentencing hearing, whether the district court would have imposed a different sentence had it known the guidelines were not mandatory, is authorized by rule or by precedent, and whether the procedure comports with this court's decision in *Booker, infra*.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES – Continued

STATUTES

OPINION BELOW

The Seventh Circuit Court of Appeals opinion is published. See, *United States v. Mitra*, 405 F.3d 492, No. 04-2328, 2005 WL 1390278 (7th Cir. 2005). The District Court's *advisory order on limited remand*, pursuant to *United States v. Paladino*, 401 F.3d 471 (7th Cir. 2005), is not published, but is available online as 2005 U.S. Dist. LEXIS 9729, affirmed by *United States v. Mitra*, 134 Fed. Appx. 963, 2005 U.S. App. LEXIS 11161 (7th Cir. Wis., June 13, 2005). All three opinions are included in the Appendix.

JURISDICTION

The Seventh Circuit filed its opinion on April 12, 2005, and issued its order affirming the district court, pursuant to the Seventh Circuit Court of Appeals *Paladino* procedure, on June 13, 2005. This Court has jurisdiction under 28 U.S.C. § 1254(1) to review the circuit court's decision on a writ of certiorari.

STATUTORY PROVISIONS INVOLVED

18 U.S.C. § 1030

(a) whoever –

(5)

(A)

(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (I), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused) –

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

shall be punished as provided in subsection © of this section.

(e) As used in this section –

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and

includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer –

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

STATEMENT OF FACTS

The Petitioner, Rajib K. Mitra, was indicted in the United States District Court for the Western District of Wisconsin on two counts of violating 18 U.S.C. § 1030(a)(5)(A) and (B), the computer fraud statute, for broadcasting signals that interfered with the Madison, Wisconsin public safety (police) radio communications system.

As can be gleaned from the appendix documents, Mitra, a graduate student at the University of Wisconsin, transmitted a radio signal that prevented the communications system for police, fire, ambulance, and other emergency communications in Madison, Wisconsin, from operating. He was prosecuted for violation of Section 1030, which is titled "Fraud and related activity in connection with computers." It is generally known as the criminal ban on computer hacking.

Mitra argued unsuccessfully in the District Court, and before the Court of Appeals, that his actions were in the nature of unauthorized broadcasts, or interference, and that Section 1030 is intended only to cover those who hack into computer servers to steal or alter information.

The Court of Appeals opinion demonstrates that, as computer chips become more ubiquitous in products ranging from police communications equipment, to cell phones and iPods, to automobiles, the scope of malicious conduct that district courts will permit to be prosecuted under Section 1030 will continue to grow.

The public safety radio frequency communications system in Madison, Wisconsin uses Motorola's Smartnet II. This spreads transmissions across 20 frequencies. Computer hardware and software assigns each conversation to an open channel, with one channel designated for control.

The Court of Appeals wrote that a signal transmitted by Mitra "blanketed all of the City's communications towers and prevented the computer from receiving, on the control channel, data essential to parcel traffic among the other 19 channels." As a result, "public safety departments

were unable to coordinate their activities because the radio system was down."

The Court explained that Mitra would "send the signals that took control of the system." Law enforcement authorities found him by using radio direction finders. They also seized Mitra's computer and radio transmission equipment.

The Court of Appeals wrote that prosecutor's theory, which the District Court accepted, "is that Smartnet II is a "computer" because it contains a chip that performs high-speed processing in response to signals received on the control channel, and as a whole is a "communications facility directly related to or operating in conjunction" with that computer chip. It is a "protected computer" because it is used in "interstate . . . communication"; the frequencies it uses have been allocated by the Federal Communications Commission for police, fire, and other public-health services.

Mitra's transmissions on Halloween included "information" that was received by the Smartnet. Data that Mitra sent interfered with the way the computer allocated communications to the other 19 channels and stopped the flow of information among public-safety officers. This led to "damage" by causing a "no system" condition citywide, impairing the "availability of . . . a system, or information" and creating "a threat to public health or safety by knocking out police, fire, and emergency communications."

The Court of Appeals wrote that Mitra's theory is that all he did was "gum up a radio system." Mitra did not hack into a computer, as the Congress intended the statute to mean. Mitra argued that if what he did violates Section 1030, then "Every cell phone and cell tower

is a "computer" under this statute's definition; so is every iPod, every wireless base station in the corner coffee shop, and many another gadgets." Reading Section 1030 to cover all of these, and police radio too, Mitra asserted, would expand the statute's coverage beyond what Congress contemplated or intended. Indeed, in its briefs, and at oral argument, the government conceded that Mitra's prosecution was a novel application of the statute.

The Court of Appeals did not discuss in detail the ramifications of this holding for a computer chip based economy. However, the Court of Appeals did go into detail on the nature of the legislative process, and legislative intent. That is, Mitra argued that the Congress could not have intended when it enacted Section 1030 over twenty years ago that it would apply to communications systems that use computer chips. But this Court of Appeals opinion, authored by Judge Easterbrook, holds that courts should not be guided by legislative intent.

Legislatures do not have intent, wrote the Court of Appeals, only individual legislators do. And, their intent is not pertinent to courts. The Court of Appeals acknowledged that neither the Congress nor legislators intended the application of Section 1030 to Mitra's acts, but the absence of such intent on the part of Congress does not matter. The Court of Appeals wrote that legislatures "write general statutes rather than enacting a list of particular forbidden acts. And it is the statutes they enacted – not the thoughts they did or didn't have – that courts must apply."

The Court of Appeals noted that there are limitations on the scope of Section 1030. There must be intentional damage. Also, the damage must be at least $5,000 or

bodily injury or danger to pubic safety. Finally, the computer must operate in interstate commerce. However, this third limitation hardly operates as a limitation. The Court of Appeals wrote that *any* use of radio frequency is interstate commerce, because radio spectrums are licensed by the Federal Communications Commission (FCC). It does not matter if the use of the spectrum is neither interstate nor commercial. By operation of law, it is interstate commerce.

The Court of Appeals noted that the spectrum used by Madison public safety entities is licensed by the FCC. The opinion is silent on what affect the use of an unlicensed spectrum would have on the interstate commerce analysis.

Mitra was sentenced before *United States v. Booker*, 125 S. Ct. 738 (2005), and did not formally argue in the District Court that the Sixth Amendment limits the judge's role in sentencing. Mitra argued in the Court of Appeals that it was unfair to impose a hard and fast rule that unless a defendant made an argument in the District Court that the Court of Appeals had already termed frivolous (that *Apprendi* applied to guidelines calculations), that review now would now be limited to a search for plain error. Indeed, the Seventh Circuit Court of Appeals, although it had invariably rejected as frivolous such *Apprendi* arguments, wrote that,

> The approach developed in *United States v. Paladino*, 401 F.3d 471 (7th Cir. 2005), applies to this sentence, which falls within a properly calculated guideline range. Accordingly, although the judgment of conviction is affirmed, we remand to the district court under the terms of *Paladino* so that the district judge may inform us whether the additional discretion provided by

Booker's remedial holding would affect Mitra's sentence.

The District Court then permitted briefing on whether the previously imposed sentence should be modified. On May 18, 2005, the District Court (the very same district judge as in *Booker*), "advised the Court of Appeals" that it would impose Mitra's original sentence "had the sentencing guidelines been merely advisory."

On June 13, 2005, the Seventh Circuit Court of Appeals, in an unpublished Rule 53 Order, affirmed the district court.

REASONS FOR GRANTING THE PETITION

I. THIS COURT SHOULD EMPLOY PRECEDENT IGNORED BY THE SEVENTH CIRCUIT AND HOLD THAT CONGRESSIONAL INTENT GIVES LOWER COURTS GUIDANCE IN DETERMINING WHETHER A CONSTRUCTION FOLLOWS FROM A STATUTE IN NOVEL PROSECUTIONS.

In this Case, the Seventh Circuit affirmatively and expressly held that if it is necessary to determine whether a person's conduct is proscribed by criminal statute, the Court's analysis need not include consideration of congressional intent in the enactment of the law.

But this Court's precedent doesn't so easily dispense with Congress. At least in the context of whether an operative fact is a sentence enhancer or an element of the crime, this Court has laid out a painstaking methodology for statutory analysis that mandates a finding of whether what Congress said trumps what Congress intended. See

Almendarez-Torres v. United States, 523 U.S. 224, 234, 235-36 (1998).

The Seventh Circuit's opinion herein is a tour de force example of the kind of judicial fact-finding that this Court has been vigorously leashing since *Apprendi v. New Jersey*, 530 U.S. 466 (2000). Ignoring what the Seventh Circuit admits is the lack of intent by Congress to expand 18 U.S.C. § 1030, into novel prosecutions that have nothing to do with Congress's intent to halt computer hacking, the Seventh Circuit herein holds that if it looks, acts, and quacks like a "protected computer" then, well, that's what Congress wrote. Why is the Seventh Circuit pounding its own square pegs when Congressional intent is so easily determined and helpful in assessing whether a novel fact situation lies within the reach of the statute?

Moreover, there is no indication that Congress has intentionally delegated to the courts the determination of whether one act or another amounts to an attack on a protected computer. See, for example, *United States v. Buckland*, 277 F.3d 1173 (2002) (Congress intentionally left to the courts the determination of the burden of proof and the fact-finder with respect to drug type and amount in § 841).

Indeed, unlike the Seventh Circuit's see no Congress, hear no Congress approach, this Court has clearly and repeatedly indicated that it *must* "look to the statute's language, structure, subject matter, context and history – factors that typically help courts determine a statute's objectives and thereby illuminate its text." *Almendarez-Torres*, 523 U.S. at 228; see also *Carter v. United States*, 530 U.S. 255, 272-74 (2000); *Castillo v. United States*, 530 U.S. 120 (2000); *Jones v. United States*, 526 U.S. 227, 232-39

(1999); *Gozlon-Peretz v. United States*, 498 U.S. 395, 404 (1990) (Congress presumed in Controled Substances Act to act intentionally and purposely in disparate inclusion or exclusion). On occassion, in determining Congressional intent, this Court has recited lengthy passages from relevant legislative history. See, *Feist Pub'lns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 355 (1991).

The Seventh Circuit's approach in this case, if permitted to stand, would mean that legislative intent would be ignored in determining whether it is possible to read a statute broadly, and whether it makes any sense to do so, but the Seventh Circuit has not always taken this approach, and it is not entirely clear why it does in this case. See, *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996), citing to *American Airlines, Inc. v. Wolens*, 513 U.S. 219, 228-29 (1995).

In the final analysis, by agreeing with the prosecution that the Computer Fraud and Abuse Act can be broadly read to criminally punish (96 month's worth in this case) acts that don't seek to hack into computer networks or obtain or change data, the Seventh Circuit Court of Appeals dispensed with the methodology of examining legislative intent, and affirmed a lengthy sentence for what has always been thought of as annoying interference. No one else has ever, and no one else has since been prosecuted for broadcasting interfering radio signals under 18 U.S.C. § 1030. No other court has held that virtually any device that contains a processor is a protected computer. This Court should grant this Petition to give the lower courts the guidance they need in determining when, if at all, a criminal prosecution is entitled to break new ground.

II. THIS COURT SHOULD RESOLVE THE SPLIT AMONG THE CIRCUITS AS TO WHETHER SENTENCES IMPOSED PRIOR TO *BOOKER* – BUT DIRECTLY APPEALED SINCE *BOOKER* – SHOULD BE VACATED OR MERELY SUBJECT TO LIMITED REMAND TO THE DISTRICT COURT FOR A NONEVIDENTIARY DETERMINATION AS TO WHETHER A DIFFERENT SENTENCE WOULD HAVE BEEN IMPOSED HAD THE GUIDELINES BEEN "ADVISORY."

After this Court's decision in *Apprendi*, supra, defendants in the Seventh Circuit's jurisdiction regularly, at least at first, filed objections to guidelines determinations not made, so the arguments went, in keeping with *Apprendi's* approach. But by the time that Mitra was sentenced, under Seventh Circuit case law an *Apprendi* objection would have been rejected out of hand as borderline frivolous. See for example, *United States v. Vallejo*, 373 F.3d 855 (2004) (*Apprendi* does not require jury to determine that defendant possessed a firearm in connection with a violent crime, increasing his offense level, where jury found only that defendant was a felon in possession of a firearm); *United States v. Johnson*, 335 F.3d 589 (7th Cir. 2003) (*per curiam*) (declining to revisit holding that *Apprendi* does not apply unless the sentence imposed "is less than the statutory maximum prescribed by the statute of conviction"; rejecting argument that *Ring v. Arizona*, 536 U.S. 584 (2002), required a different result); *United States v. Holman*, 314 F.3d 837, 846 (7th Cir. 2002), *cert. denied*, 123 S. Ct. 2238 (2003) (*Apprendi* does not require jury to determine facts underlying sentencing enhancements, including obstruction); *United States v. Knox*, 301 F.3d 616, 620 (7th Cir. 2002) ("*Apprendi* is never relevant to guidelines calculations").

In countless unpublished *Anders*[1] decisions, the Seventh Circuit found that any potential *Apprendi* complaints regarding application of the guidelines based upon facts found by sentencing courts by a preponderance of the evidence were *frivolous*. See *United States v. Coles*, No. 03-1451 (7th Cir. May 3, 2004); *United States v. Trenton*, No. 02-3168 (7th Cir. April 28, 2003); *United States v. Jackson*, No. 01-2332, Slip Op. at 10-11 (7th Cir. June 20, 2002) (*Apprendi* argument would be frivolous).

Understandably, Mitra (sentenced before *Blakely v. Washington*, 124 S. Ct. 2531 (2004)), made no formal *Apprendi* argument. Incredibly, the Seventh Circuit, after *Booker*, decided that if a defendant had not made the (by then frivolous) *Apprendi* argument to the application of the guidelines determinations, sentences would only be reviewed for plain error, which could only be determined by use of a limited remand to the District Court for the purpose of having the original sentencing judge advise the Court of Appeals whether, had the guidelines been advisory at the time of the original sentencing, the sentence would have been any different. See, *United States v. Paladino*, 401 F.3d 471, 484 (7th Cir. 2005). The dissent in *Paladino* termed this approach *unprincipled*. 401 F.3d at 487 (Ripple, Judge, dissenting).

The significance of the Seventh Circuit's approach is that the defendant has the burden of proving plain error, whereas the government has the burden of proving harmless error. *United States v. Olano*, 507 U.S. 725, 734-35

---

[1] *Anders v. California*, 386 U.S. 738 (1967). These decisions are not cited for precedent, but to illustrate the state of the art in the Seventh Circuit.

(1993). The Seventh Circuit's approach is apparently in accord with that approved in the District of Columbia, and Second Circuit. *United States v. Crosby*, 397 F.3d 103 (2nd Cir. 2005); *United States v. Coles*, 403 F.3d 764 (D.C. Cir. 2005) (per curiam).

In a virtual compendium of the approaches in the various circuits, the Eight Circuit, in specifically criticizing the *Paladino* procedure, wrote that,

> Though creative, we conclude that this approach violates the Supreme Court's command in *Booker* that courts of appeals apply "*ordinary* prudential doctrines," including "*the* 'plain-error' test." 125 S. Ct. at 769 (emphasis added).

United States v. Pirani, 406 F.3d 543, 552 (8th Cir. 2005), citing to *United States v. Booker*, 125 S. Ct. 738, 769 (2005). The *Pirani* court indicates that the Eight Circuit's approach is in accord with that established in the Eleventh, the First, and the Fifth Circuits. The Third, Fourth, and Sixth Circuits are in yet a third camp. See *United States v. Davis*, 407 F.3d 162 (3rd Cir. 2005) (en banc); *United States v. Hughes*, 401 F.3d 540 (4th Cir. 2005); *United States v. Oliver*, 397 F.3d 369 (6th Cir. 2005).

While these differences may be temporal (eventually all the pre-*Blakely* sentencings will reach finality) they are deep and real. The problem with the Seventh Circuit's approach, in addition to conflicting with the several mentioned circuits, is that neither Fed. R. Crim. P. Rule 52(b) nor this Court's plain error decisions authorize a remand for development of the record with respect to whether the newly complained of sentencing error affected substantial rights. The *Paladino* review clearly abdicates (maybe avoids) assessing prejudice, which is the job of the

reviewing court. See *United States v. Dominguez Benitez*, 124 S. Ct. 2333, 2340 (2004). Mitra believes, as above, that review is necessary to give guidance to the lower courts in so-called *Booker* procedures, and to resolve these profound conflicts.

CONCLUSION

This Court should grant the petition for a writ of certiorari and reverse the decision of the Seventh Circuit Court of Appeals.

Respectfully submitted,

ROBERT G. LEBELL
KOSTICH, LEBELL, DOBROSKI
& MORGAN LLP
735 West Wisconsin Avenue, #800
Milwaukee, WI 53233-2413
Phone: (414) 276-1233
Fax: (414) 276-5874
Email: dorbell@execpc.com

UNPUBLISHED ORDER
Not to be cited per Circuit Rule 53

United States Court of Appeals
For the Seventh Circuit
Chicago, Illinois 60604

June 13, 2005

Before

Hon. FRANK H. EASTERBROOK, Circuit Judge

Hon. DIANE P. WOOD, Circuit Judge

Hon. DIANE S. SYKES, Circuit Judge

UNITED STATES OF AMERICA, *Plaintiff-Appellee,* **No.** 04-2328 **v.** RAJIB K. MITRA, *Defendant-Appellant.*	Appeal from the United States District Court for the Western District of Wisconsin. No. 03-CR-153-S John C. Shabaz, *Judge*

Order

After concluding that the district court had correctly calculated the range under the Sentencing Guidelines, this court ordered a limited remand so that the district court could state on the record whether the sentence remains appropriate now that *United States v. Booker*, 125 S. Ct. 738 (2005), has limited the Guidelines to advisory status. See *United States v. Paladino*, 401 F.3d 471 (7th Cir. 2005).

The district judge has replied that he would today impose the same sentence, knowing of the Guidelines' advisory status. The range under the Guidelines is 87 to 108 months, and Mitra's sentence of 96 months is slightly

below its mid-point. We do not see any reason why such a sentence would be deemed "unreasonable" in post-*Booker* practice. The judgment of the district court therefore is affirmed

In the

United States Court of Appeals

For the Seventh Circuit

No. 04-2328

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

RAJIB K. MITRA,

Defendant-Appellant.

Appeal from the United States District Court
for the Western District of Wisconsin.
No. 03-CR-153-S – **John C. Shabaz**, *Judge.*

ARGUED FEBRUARY 16, 2005 – DECIDED APRIL 18, 2005

Before EASTERBROOK, WOOD, and SYKES, *Circuit Judges.*

EASTERBROOK, *Circuit Judge.* Wisconsin's capital city uses a computer-based radio system for police, fire, ambulance, and other emergency communications. The Smartnet II, made by Motorola, spreads traffic across 20 frequencies. One is designated for control. A radio unit (mobile or base) uses the control channel to initiate a conversation. Computer hardware and software assigns the conversation to an open channel, and it can link multiple roaming units into "talk groups" so that officers in the field can hold joint conversations. This is known as

a "trunking system" and makes efficient use of radio spectrum, so that 20 channels can support hundreds of users. If the control channel is interfered with, however, remote units will show the message "no system" and communication will be impossible.

Between January and August 2003 mobile units in Madison encountered occasional puzzling "no signal" conditions. On Halloween of that year the "no system" condition spread citywide; a powerful signal had blanketed all of the City's communications towers and prevented the computer from receiving, on the control channel, data essential to parcel traffic among the other 19 channels. Madison was hosting between 50,000 and 100,000 visitors that day. When disturbances erupted, public safety departments were unable to coordinate their activities because the radio system was down. Although the City repeatedly switched the control channel for the Smartnet system, a step that temporarily restored service, the interfering signal changed channels too and again blocked the system's use. On November 11, 2003, the attacker changed tactics. Instead of blocking the system's use, he sent signals directing the Smartnet base station to keep channels open, and at the end of each communication the attacker appended a sound, such as a woman's sexual moan.

By then the City had used radio direction finders to pin down the source of the intruding signals. Police arrested Rajib Mitra, a student in the University of Wisconsin's graduate business school. They found the radio hardware and computer gear that he had used to monitor communications over the Smartnet system, analyze how it operated, and send the signals that took control of the system. Mitra, who in 2000 had received a B.S. in computer

science from the University, possessed two other credentials for this kind of work: criminal convictions (in 1996 and 1998) for hacking into computers in order to perform malicious mischief. A jury convicted Mitra of two counts of intentional interference with computer-related systems used in interstate commerce. See 18 U.S.C. §1030(a)(5). He has been sentenced to 96 months' imprisonment. On appeal he says that his conduct does not violate §1030 – and that, if it does, the statute exceeds Congress's commerce power.

Section 1030(a)(5) provides that whoever

(A)

> (i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused) –

> (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss

> resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
>
> (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
>
> (iii) physical injury to any person;
>
> (iv) a threat to public health or safety; or
>
> (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security . . .
>
> shall be punished as provided in subsection (c) of this section.

Subsection (e)(1) defines "computer" as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device". Subsection (e)(2)(B) defines a "protected computer" to include any computer "used in interstate or foreign commerce or communication". Finally, subsection (e)(8) defines "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information".

The prosecutor's theory is that Smartnet II is a "computer" because it contains a chip that performs high-speed processing in response to signals received on the control channel, and as a whole is a "communications

facility directly related to or operating in conjunction" with that computer chip. It is a "protected computer" because it is used in "interstate . . . communication"; the frequencies it uses have been allocated by the Federal Communications Commission for police, fire, and other public-health services. Mitra's transmissions on Halloween included "information" that was received by the Smartnet. Data that Mitra sent interfered with the way the computer allocated communications to the other 19 channels and stopped the flow of information among public-safety officers. This led to "damage" by causing a "no system" condition citywide, impairing the "availability of . . . a system, or information" and creating "a threat to public health or safety" by knocking out police, fire, and emergency communications. See §1030(a)(5)(A)(i), (B)(iv). The extraneous sounds tacked onto conversations on November 11 also are "information" sent to the "protected computer," and produce "damage" because they impair the "integrity" of the official communications. This time subsection §1030(a)(5)(B)(v) is what makes the meddling a crime, because Mitra hacked into a governmental safety-related communications system.

Mitra concedes that he is guilty if the statute is parsed as we have done. But he submits that Congress could not have intended the statute to work this way. Mitra did not invade a bank's system to steal financial information, or erase data on an ex-employer's system, see *United States v. Lloyd*, 269 F.3d 228 (3d Cir. 2001), or plaster a corporation's web site with obscenities that drove away customers, or unleash a worm that slowed and crashed computers across the world, see *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991), or break into military computers to scramble a flight of interceptors to meet a

nonexistent threat, or plant covert programs in computers so that they would send spam without the owners' knowledge. All he did was gum up a radio system. Surely that cannot be a federal crime, Mitra insists, even if the radio system contains a computer. Every cell phone and cell tower is a "computer" under this statute's definition; so is every iPod, every wireless base station in the corner coffee shop, and many another gadget. Reading §1030 to cover all of these, and police radio too, would give the statute wide coverage, which by Mitra's lights means that Congress cannot have contemplated such breadth.

Well of course Congress did not contemplate or intend this particular application of the statute. Congress is a "they" and not an "it"; a committee lacks a brain (or, rather, has so many brains with so many different objectives that it is almost facetious to impute a joint goal or purpose to the collectivity). See Kenneth A. Shepsle, *Congress is a "They," Not an "It": Legislative Intent as Oxymoron*, 12 Int'l Rev. L. & Econ. 239 (1992). Legislation is an objective text approved in constitutionally prescribed ways; its scope is not limited by the cerebrations of those who voted for or signed it into law.

Electronics and communications change rapidly, while each legislator's imagination is limited. Trunking communications systems came to market after 1984, when the first version of §1030 was enacted, and none of the many amendments to this statute directly addresses them. But although legislators may not know about trunking communications systems, they *do* know that complexity is endemic in the modern world and that each passing year sees new developments. That's why they write general statutes rather than enacting a list of particular forbidden acts. And it is the statutes they enacted – not the thoughts

they did or didn't have – that courts must apply. What Congress would have done about trunking systems, had they been present to the mind of any Senator or Representative, is neither here nor there. See *West Virginia University Hospitals, Inc. v. Casey*, 499 U.S. 83, 100-01 (1991).

Section 1030 is general. Exclusions show just *how* general. Subsection (e)(1) carves out automatic typewriters, typesetters, and handheld calculators; this shows that other devices with embedded processors and software are covered. As more devices come to have built-in intelligence, the effective scope of the statute grows. This might prompt Congress to amend the statute but does not authorize the judiciary to give the existing version less coverage than its language portends. See *National Broiler Marketing Ass'n v. United States*, 436 U.S. 816 (1978). What protects people who accidentally erase songs on an iPod, trip over (and thus disable) a wireless base station, or rear-end a car and set off a computerized airbag, is not judicial creativity but the requirements of the statute itself: the damage must be intentional, it must be substantial (at least $5,000 or bodily injury or danger to public safety), and the computer must operate in interstate or foreign commerce.

Let us turn, then, to the commerce requirement. The system operated on spectrum licensed by the FCC. It met the statutory definition because the interference affected "communication." Mitra observes that his interference did not affect any radio system on the other side of a state line, yet this is true of many cell-phone calls, all of which are part of interstate commerce because the electromagnetic spectrum is securely within the federal regulatory domain. See, e.g., *Radovich v. National Football League*, 352 U.S. 445, 453 (1957); *Federal Radio Commission v.*

Nelson Brothers Bond & Mortgage Co., 289 U.S. 266, 279 (1933). Congress may regulate all channels of interstate commerce; the spectrum is one of them. See *United States v. Lopez*, 514 U.S. 549, 558 (1995); *United States v. Morrison*, 529 U.S. 598, 608-09 (2000). Mitra's apparatus was more powerful than the Huygens probe that recently returned pictures and other data from Saturn's moon Titan. Anyway, the statute does not ask whether the person who caused the damage acted in interstate commerce; it protects computers (and computerized communication systems) used in such commerce, no matter how the harm is inflicted. Once the *computer* is used in interstate commerce, Congress has the power to protect it from a local hammer blow, or from a local data packet that sends it haywire. (Indeed, Mitra concedes that he could have been prosecuted, consistent with the Constitution, for broadcasting an unauthorized signal. See 47 U.S.C. §301, §401(c).) Section 1030 is within the national power as applied to computer-based channel-switching communications systems.

Mitra offers a fallback argument that application of §1030 to his activities is so unexpected that it offends the due process clause. But what cases such as *Bouie v. Columbia*, 378 U.S. 347 (1964), hold is that a court may not apply a clear criminal statute in a way that a reader could not anticipate, or put a vague criminal statute to a new and unexpected use. Mitra's problem is not that §1030 has been turned in a direction that would have surprised reasonable people; it is that a broad statute has been applied *exactly as written*, while he wishes that it had not been. There is no constitutional obstacle to enforcing broad but clear statutes. See *Rogers v. Tennessee*, 532 U.S. 451, 458-62 (2001) (discussing *Bouie*'s rationale and limits).

The statute itself gives all the notice that the Constitution requires.

During deliberations the jury inquired about the meaning of the word "intentionally." The judge referred them to the instructions, which included a definition. Mitra says that the judge should have drafted a new definition, because the first must have been confusing (though he concedes that it was correct). This sort of problem is one for the district judge to resolve on the spot; there would be little point in Monday morning quarterbacking.

Sentencing requires but little discussion. The district judge added offense levels under U.S.S.G. §2B1.1(b)(13)(A)(iii) and (B) after concluding that Mitra had disrupted a "critical infrastructure". (Our citations are to the 2003 Manual, which the district judge used; the current version is substantively identical but numbered a little differently.) Application Note 12 defines that term; Mitra concedes that an emergency radio system fits the definition. Emergency services are one of the note's examples. Once again his argument takes the form that the authors of this language just couldn't have meant what they said. It is not as if the note were a linguistic garble, or that it is impossible to fathom why any sane person would think that the penalty for crippling an emergency-communication system on which lives may depend should be higher than the penalty for hacking into a web site to leave a rude message. The district judge was right to apply the guideline and note as written.

Mitra was sentenced before *United States v. Booker*, 125 S. Ct. 738 (2005), and did not argue in the district court that the sixth amendment limits the judge's role in

sentencing. Review now is limited to a search for plain error. The approach developed in *United States v. Paladino*, 401 F.3d 471 (7th Cir. 2005), applies to this sentence, which falls within a properly calculated guideline range. Accordingly, although the judgment of conviction is affirmed, we remand to the district court under the terms of *Paladino* so that the district judge may inform us whether the additional discretion provided by *Booker*'s remedial holding would affect Mitra's sentence.

A true Copy:

Teste:

Clerk of the United States Court of Appeals for the Seventh Circuit

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v.

RAJIB MITRA,

Defendant.

MEMORANDUM and ORDER

03-CR-153-S-01

(Filed May 18, 2005)

Presently pending before the Court in the above entitled matter is a limited remand from the United States Court of Appeals for the Seventh Circuit to determine whether this Court would impose defendant's original sentence had the sentencing guidelines been merely advisory. In *U.S. v. Paladino*, 401 F. 3d 471, 484 (7th Cir. 2005), the Court advised as follows:

> Upon reaching its decision (with or without a hearing) whether to resentence, the District Court should either place on the record a decision not to resentence with an appropriate explanation," *United States v. Crosby, supra*, 397 F. 3d at 1920, or inform this Court of its desire to resentence the defendant.

The Court has considered the views of counsel, the advisory sentencing guidelines, the purposes of sentencing and the reasons for its original sentence, determining that it would impose the same sentence.

As justification for its original sentence the Court considered the following facts:

Defendant was responsible for interrupting Madison police communications on 36 separate occasions since January 2003. Defendant used his knowledge and expertise of computers and radios to transmit radio signals that caused substantial damage to the City of Madison's emergency radio system in October and November 2003. Public health and safety were threatened because the signals interrupted communications for Madison's emergency systems. Defendant's conduct caused a substantial disruption of a critical infrastructure. Defendant on numerous occasions committed perjury by stating that the disruptions to the radio transmissions were malfunctions and not intentional. The transmissions were intentional, major and substantial damage to the radio network.

Defendant's offense level was enhanced to 24 by the Court's finding by a preponderance of the evidence that he had substantially disrupted a critical infrastructure. It was also enhanced two levels for obstruction of justice and two levels for Mitra's use of a special skill. Based on this offense level of 28 and Mitra's criminal history category of two, the advisory guideline imprisonment range is 87-108 months. The Court declined to depart upward from the guidelines and sentenced Mitra to 96 months in prison.

The imposition of the original sentence considered those suggestions presented both then and now by counsel: the seriousness of the offenses, adequate deterrence to criminal conduct, protecting the public and the defendant's lack of remorse. Had the guidelines been advisory, this Court would have imposed the same sentence believing it to be reasonable considering the defendant's criminal conduct, sufficient to hold defendant accountable and to protect the community from further criminality on his part.

Pursuant to 18 U.S.C. § 3553 the Court may consider the character and history of the defendant. As his counsel argued at sentencing defendant is a young man who worked gainfully in the computer field and pursued his master's degree. This is counterbalanced by his continuing lack of remorse and refusal to accept responsibility for his criminal conduct.

Considering all these factors, a sentence in the middle of the advisory guidelines is reasonable and necessary for the statutory purposes of sentencing.

For the reasons stated this Court advises the United States Court of Appeals for the Seventh Circuit that it would impose defendant's original sentence had the sentencing guidelines been merely advisory.

Entered this 18th day of May, 2005.

BY THE COURT:

/s/ _____
JOHN C. SHABAZ
District Judge